UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The premises located at or near to 150 Jefferson Street, Eugene, OR, 97402, a backpack, and the person of Brandon Knight, as further described in Attachment A

Case No. 6:21-mc-766

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

The premises located at or near to 150 Jefferson Street, Eugene, OR, 97402, a backpack, and the person of Brandon Knight, as further described in Attachment A hereto.

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 875(c)	Transmitting threats in interstate commerce

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Natalie R. Stewart, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone at 5:13pm a.m./p.m. *(specify reliable electronic means)*.

Date: July 6, 2021

Judge's signature

City and state: Eugene, Oregon

Mustafa T. Kasubhai, U.S. Magistrate Judge
Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF NATALIE R. STEWART

Affidavit in Support of an Application Under Rule 41 for a Search Warrant

I, Natalie R. Stewart, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am Special Agent with the Federal Bureau of Investigation (FBI), and have been so employed for approximately four years. My current responsibilities include the investigation of national security matters, to include both international terrorism and domestic terrorism.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search a tent located in the Washington Jefferson Park at 150 Jefferson St., Eugene, OR 97402 (hereinafter "Premises"), as well as a black backpack belonging to Brandon Knight ("Knight") located at or near the Premises, and the person of Brandon Knight, as described in Attachment A hereto, for evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 875(c) (hereinafter "Target Offense"). As set forth below, I have probable cause to believe that such property and items, as described in Attachment B hereto, including any digital devices or electronic storage media, are currently located in the tent described in Attachment A and located at the Washington Jefferson Park at 150 Jefferson St., Eugene, OR 97402, as well as on the person of Knight, or in the black backpack detailed in Attachment A.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement

officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. **Title 18, United States Code, Section 875(c)** provides:

(c) Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.

Statement of Probable Cause[1]

5. On July 6, 2021, I received information from the FBI Eugene Resident Agency indicating that Brandon Knight was residing at the Premises. The remaining details of my investigation are outlined below.

---

[1] Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *IP address*. The Internet Protocol address (or simply "IP address") is a unique numeric address used by digital devices on the Internet. Every digital device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that digital device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some digital devices have static—that is, long-term—IP addresses, while other digital devices have dynamic—that is, frequently changed—IP addresses.

b. *Internet*. The Internet is a global network of digital devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. *Storage medium*. A storage medium is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

6. On or about June 11 and 17, 2021, Brandon KNIGHT, while in Oregon and using the moniker "Ibrahim Al-Amreeki," communicated threats via Facebook to an FBI Online Covert Employee (OCE). Specifically, KNIGHT sent messages indicating his intent to kill his wife and his intent to "hunt down and execute individuals who work on behalf of the FBI."

7. On or about August 30, 2020, Brandon KNIGHT was arrested in Flagstaff, Arizona, on multiple counts of disorderly conduct, resisting arrest and aggravated assault on a Police Officer. According to an Officer Safety Bulletin distributed by the Pima County Sheriff's Department, related to this arrest, KNIGHT made threats directly to law enforcement by stating "that if law enforcement intervened with him and [Adult Victim 1 (AV1)], he would kill the police and would be glorified for doing so."

8. Based on police reports from the University of Arizona Police Department (UAPD), on or about December 4, 2020, in response to a report of a domestic violence assault in progress, UAPD officers arrested KNIGHT in Tucson, Arizona, on multiple charges including domestic violence assault and aggravated assault on a Peace Officer. A bystander witnessed KNIGHT beating and kicking a female victim who was on the ground. According to a UAPD report, when the bystander intervened, KNIGHT pulled out a knife, but put it away when he realized the bystander was not a police officer. Officers arrived and when they attempted to place KNIGHT under arrest, KNIGHT forcibly resisted, spit at the officers, grabbed and pinched one of the officers, and appeared to have grabbed for one of the officer's taser. During the incident, KNIGHT stated that he could be COVID positive because his brother was COVID positive while helping KNIGHT three days earlier. While being arrested KNIGHT continuously spit and coughed while yelling profanity and threatening statements towards the officers on the scene to

include "get COVID on all you bitches ... let it kill your family, grandmothers, mothers, children…you fucking scumbags." While being transported from the scene to the jail, KNIGHT made verbal threats to law enforcement, stating he would wait for the officers to be off duty to kill them and that he would come to UAPD to retrieve his property and "do something." KNIGHT further stated he got pleasure from hearing about police officers being murdered around the country and would wait for them to be off duty, without their guns to kill them.

9. Based on a Tucson Police Department (TPD) incident report, on or about December 20, 2020, the TPD received a 911 call and was dispatched to a Circle K Convenience Store & Gas Station in response to a report of domestic violence with a weapon. According to the report, the incident involved a fight between AV1 and Brandon KNIGHT. A witness observed KNIGHT kick AV1. When AV1 then attempted to leave the scene, AV1 pushed KNIGHT. In response, KNIGHT lifted his shirt and brandished a shiny object in his waistband. Both KNIGHT and AV1 refused to speak to TPD officers when questioned. They were both transported and booked into Pima County jail. KNIGHT was arrested for Domestic Violence-Assault and Domestic Violence-Threats. AV1 was arrested for Domestic Violence-Assault.

10. At some point between January 2021 and June 2021, KNIGHT traveled from Arizona to Oregon. Due to an ongoing FBI investigation, on or about May 14, 2021, an FBI OCE friended a Facebook account believed to be operated by KNIGHT. Subsequent records from Facebook indicated the registered email accounts for the Facebook account were knightbrandon43@yahoo.com and Brandon.knight.353250@facebook.com. Additionally, the credit card on file was in the name of Brandon Knight.

11. FBI OCE engaged in online communications with KNIGHT via Facebook Messenger. On or about May 19, 2021, FBI OCE received a video from KNIGHT showing an unidentified person video recording themselves and another unidentified person riding in between freight train railcars. KNIGHT and OCE stated the following related to the video:

OCE: what is this? is that you now?

Al-Amreeki: On a train hahahhaa not a passenger but freight train.

OCE: I see that, where are you going?

Al-Amreeki: In Oregon now.

OCE: Wow, be careful man.

Al-Amreeki sent another video that'll be labeled below as Video#2.

OCE: Who is that person?

Al-Amreeki: Wife. I missing 3 others lol hahahaha Allahu akbar, [Allah is great].

13. Based on Eugene, Oregon Police Department (EPD) incident reports, on or about June 11, 2021 at approximately 07:50 AM, the EPD responded to a homeless encampment at approximately West 5th Avenue & Jefferson Street, Eugene, Oregon to investigate a report of a dispute. Upon arrival, Adult Victim 2 (AV2)[2] and AV1 were present. AV2 told the officer that KNIGHT grabbed an axe and swung it around while saying he was going to kill AV2 and AV1 and "chop them into little pieces." AV2 also told the officer that KNIGHT was mentally ill and threatened to kill any police who arrived. AV2 stated a male bystander took the axe away from KNIGHT and KNIGHT left, but was still texting AV2 on a messaging application using the user name "Ibrahim."

[2] Based on information provided by the Portland Police Department, AV2 has used a false name in connection with interactions with law enforcement.

14. Based on EPD incident reports, on or about June 11, 2021 at approximately 12:58 PM, EPD responded again to the same area of West 5th Avenue & Jefferson Street and an officer interviewed AV2. AV2 stated KNIGHT swiped at her tent with a knife but did not damage it. The officer then interviewed AV1. AV1 advised that KNIGHT was her husband, although they were never legally married but had been together since 2017. AV1 stated KNIGHT "came at" AV1 and AV2 earlier with an axe and she was scared of him. AV1 provided the officer with KNIGHT's phone number, 541-583-3375 (Subject Phone 1). The officer interviewed witness 1 (W1), in a neighboring tent. W1 indicated KNIGHT was there with a knife prior to the police arrival. W1 describe the knife as a small, approximately a three-inch blade.

15. On the same day as the above incidents, on or about June 11, 2021 at approximately 3:24pm CST, KNIGHT engaged in a conversation with the FBI OCE via Facebook Messenger utilizing the same Facebook account "Ibrahim Al-Amreeki". At the time of the communications, the OCE was in the Northern District of Illinois and had no knowledge of the above EPD involved incidents. The following conversation took place:

OCE: How are you?

Al-Amreeki: I'm doing horrible

OCE: La hawla wla quata illa billah, [There is no power but from Allah] why?[3]

Al-Amreeki: An individual needs to die

Al-Amreeki: And I might become a Shahid [martyr] tonight

OCE: What???

[3] The majority of the communications were in English but in the limited instances where Arabic words or phrases were spoken or written, the preserved conversations have been translated by FBI linguists and are contained in brackets.

OCE: Why?

Al-Amreeki: May Allah accept it

Al-Amreeki: I'm fully armed and ready to go to battle

Al-Amreeki: I hope that Allah gives me Gardens beneath which rivers flow

OCE: Please pray istikhara prayer before you do anything, you need to calm down and tell me what's going on. [Istikhara prayer is Arabic for Guidance seeking prayer].

OCE: Akhi

OCE: Are [you] still there akhi?

Al-Amreeki: Yrs [*sic*]

Al-Amreeki: Make Dua [pray for me]

OCE: I will, but tell me what's going on. [Al-Amreeki loved OCE's message above]

Al-Amreeki: I am not able to find it

OCE: Find what??

OCE: What are you looking for?

Al-Amreeki: Suicide

OCE: Akhi, you need to make the Istikhara prayer. What suicide? that's haram [forbidden]. Please tell me what are you talking about.

OCE: I'm really worried about you akhi.

OCE: Please talk to me.

OCE: Akhi, I understand becoming a martyr is every Muslim's dream, but suicide is not the answer.

Al-Amreeki: Suicide is intentional when you go into the path of the martyrs sword [*sic*]

OCE: Suicide is not the same as martyrdom, akhi.

OCE: Listen akhi, if you're planning something, I may be able to help you so your effort will be recognized [by] the Mu'min [believers] all over the world.

Al-Amreeki: Ameen [Amen]

OCE: But you still did not tell me what are you planning on doing.

OCE: Don't just waste your life in vain.

OCE: Akhi, is your plan is a personal matter or in the sake of Allah?

OCE: Akhi Ibrahim.

Al-Amreeki: My plan is to kill my wife

OCE: La hawla wla quata illa billah, why akhi? [There is no power but from Allah].

OCE: You said she was a Muslim.

Al-Amreeki: Zina [Adultery]

Based on the context of this conversation and the information from the police reports described above, I believe that Knight was referring to AV1 when he stated he planned to kill his wife.

16. On June 11, 2021, Facebook provided records in response to an emergency request pursuant to 18 U.S.C. § 2702. According to those records, IP address 2607:fb90:8228:a820:0000:0006:12ba:b901 (the "b901 IP address") was being used to access the Facebook profile "Al-Amreeki", UID 100002048415041 on June 11, 2021 at 21:54:05 UTC. This time translates to 3:54:05 PM CST which corresponded with the above FBI OCE communications.

17. Based on open source IP attribution lookup, the b901 IP address belonged to T-Mobile. T-Mobile provided records in response to an emergency request pursuant to 18 U.S.C. §

2702. According to T-Mobile records, the account subscriber for the b901 IP address on June 11, 2021, was Brandon KNIGHT. According to T-Mobile, the IP address was associated with an account for a device listed as an "LG STYLO6 64G WHT TMUS KIT RSU." Based on open source searches, this designation corresponds with a LG Stylo 6, 64 gigabyte, white mobile phone. Additionally, T-Mobile records the phone number 541-538-3375 and IMSI 310260042917969 are assigned to that phone. According to T-Mobile records for phone number 541-538-3375, GPS data indicated that on or about June 11, 2021 at approximately 11:44:26 PM PDT, the phone was located at 44.054521, -123.101120 which corresponded with the Washington Jefferson Park, in Eugene Oregon, within 88 meters or 289 feet around West 5th Avenue and Jefferson Street in Eugene, Oregon. This is the park in which the Premises is located.

18. In response to the location information provided by the T-Mobile records, EPD officers went to the Washington Jefferson Park and saw a light move in the tent that was previously identified by AV2 as belonging to KNIGHT. Officers located and identified KNIGHT and effectuated an arrest of KNIGHT.

19. KNIGHT was arrested by EPD for "Menacing – Threats" and on an outstanding warrant from Pima County, Arizona. The Eugene, Oregon authorities did not file charges. KNIGHT was subsequently released from custody on June 16, 2021.

20. After his release, KNIGHT again engaged in a conversation with a FBI OCE on or about June 17, 2021. The following conversation took place:

Al-Amreeki: I was arrested

OCE: Hey akhiiiiii, what happened?

Al-Amreeki: The FBI was tracking my location

OCE: ok??

Al-Amreeki: Declaration of war

OCE: What do you mean?

OCE: Are you out now?

OCE: Akhi.

OCE: Are you still there?

OCE: Akhi

Al-Amreeki: Yes

Al-Amreeki: They arrested me when I left the Masjid [Mosque].

OCE: Tell me the story, what happened tp you and what happened with your wife?

OCE: *To you [corrected the above typo].

Al-Amreeki: They charge me as a fugitive from Justice

OCE: And what now?? Are you still in prison?

Al-Amreeki: My wife was raped

Al-Amreeki: I declare war on the United States government

Al-Amreeki: Hunt down any person working for the FBI

OCE: la hawla wla quwata illa billah [There is no power but from Allah]

Al-Amreeki: Even if they go to the Masjid [Mosque]

Al-Amreeki: Allah says do not spy on your Muslim brother so if they're spying on their Muslim brother they deserve to be executed

Further on in the conversation the following was stated:

OCE: I am sorry to hear that

Al-Amreeki: So now I'm on a mission to hunt down and execute individuals who work on behalf of the FBI

OCE: So are you now released?

Al-Amreeki: Yes

OCE: Alhamdu lillah

Al-Amreeki: But my phone is being hacked and tracked

Al-Amreeki: By the United States government

Al-Amreeki: So that they're listening in on us right now I want him to know that there is no God except one and his name is Allah and that Prophet Muhammad is the final messenger and the seal of all the prophets peace be upon all of them

Al-Amreeki: And to make me a Shahid [martyr]

OCE: Ameen ya rab alalameen [Amen O Lord of the universe]

Al-Amreeki: Take me to cut my head off just like I'll cut theirs off

Al-Amreeki: They can cut my head off just like I will cut their heads off

Al-Amreeki: Let it glow like gold on the day of judgement AMEEN [Amen]

Further conversation contained the following:

Al-Amreeki: The last thing they'll be begging for is the mercy of Allah

Al-Amreeki: I'm already tracking the FBI agent who track me

21. On July 6, 2021, the FBI Eugene Resident Agency performed physical surveillance of Brandon Knight near the area of the Washington Jefferson Park in Eugene, OR. FBI Eugene special agents observed Knight walking with a black backpack near and into the

Premises. An FBI Eugene special agent observed the backpack to be small to medium in size, with bungee cords strapped to it, and an item protruding from the backpack that appeared to be a metal pole or bar. Agents observed Knight enter and leave the Premises a number of times while surveilling the area.

22. Based on the threatening messages contained in these conversations, Knight's record of threats and actual physical violence against AV1 and others, and the events of June 11, 2021, I believe that the Premises and Knight's person contain evidence of the above-described offense.

Electronic Records

23. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One form in which the records will likely be found is data stored on a computer's hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to as digital devices). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

24. There is probable cause to believe, and I do believe, that records will be stored on a digital device in the Premises, on Knight's person, or in the backpack.

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person "deletes" a file on a digital device, the data contained in the file does not actually

disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

d. Based on actual inspection of other evidence related to this investigation, I am aware that there is probable cause to believe that digital devices were used to send the threatening communications detailed above. Thus, there is reason to believe that there is a digital device currently located on the Premises, in the backpack, or on Knight's Person.

25. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this

forensic electronic evidence will be on any digital device in the Premises, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This "timeline"

information may tend to either inculpate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is

not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a digital device to commit a crime such as to send threatening communications via email, the individual's digital device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I know that a digital device used to commit a crime of this type may contain: data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

26. Because more than one person may share the Premises as a residence, it is possible that the Premises will contain digital devices that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those digital devices, the warrant applied for would permit the seizure and review of those items as well.

27. In most cases, a thorough search of the Premises for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the Premises or Knight's Person, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking

of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

Nature of Examination

28. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

29. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

30. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

31. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

32. If a computer or storage media contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain that computer or storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

33. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Conclusion

34. Based on the foregoing, I have probable cause to believe, and I do believe, Brandon Knight violated Title 18 U.S.C. Section 875(c), and that evidence of that offense, as more fully described in Attachment B hereto, is presently located at the Premises, in Knight's backpack, and on Knight's person which are more fully described above and in Attachment A hereto. I therefore request that the Court issue a warrant authorizing a search of the Premises, the backpack, and Knight's person, as described in Attachment A for the items listed in Attachment B and the examination and seizure of any such items found.

35. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) William M. McLaren, and AUSA McLaren advised me that in his opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

Request for Sealing

36. I further request that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrant, including the application, this affidavit, the attachments, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may endanger the life or physical safety of an individual, cause flight from prosecution, cause destruction of or tampering with evidence, cause intimidation of potential witnesses, or otherwise seriously jeopardize an

/ / /

/ / /

/ / /

/ / /

/ / /

investigation. Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation.

/s/ Natalie R. Stewart, Per Rule 4.1
NATALIE R. STEWART
Special Agent, FBI

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 5:13pm a.m/p.m. on July 6, 2021.

MUSTAFA T. KASUBHAI
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

1. The Premises to be searched is a tent located in the Washington Jefferson Park, at 150 Jefferson St, Eugene, OR, 97402. The tent is located near under the Interstate-105 overpass in an encampment with other tents. The tent has a dark gray and light green two-toned exterior. It features a rainfly over its primary entrance that comes to a point, and it is located directly next to a smaller tent that is light blue in color. Figure 1 depicts the exterior of the Premises tent Figure 2 depicts an overhead view of the park and the above-named overpass.

Figure 1

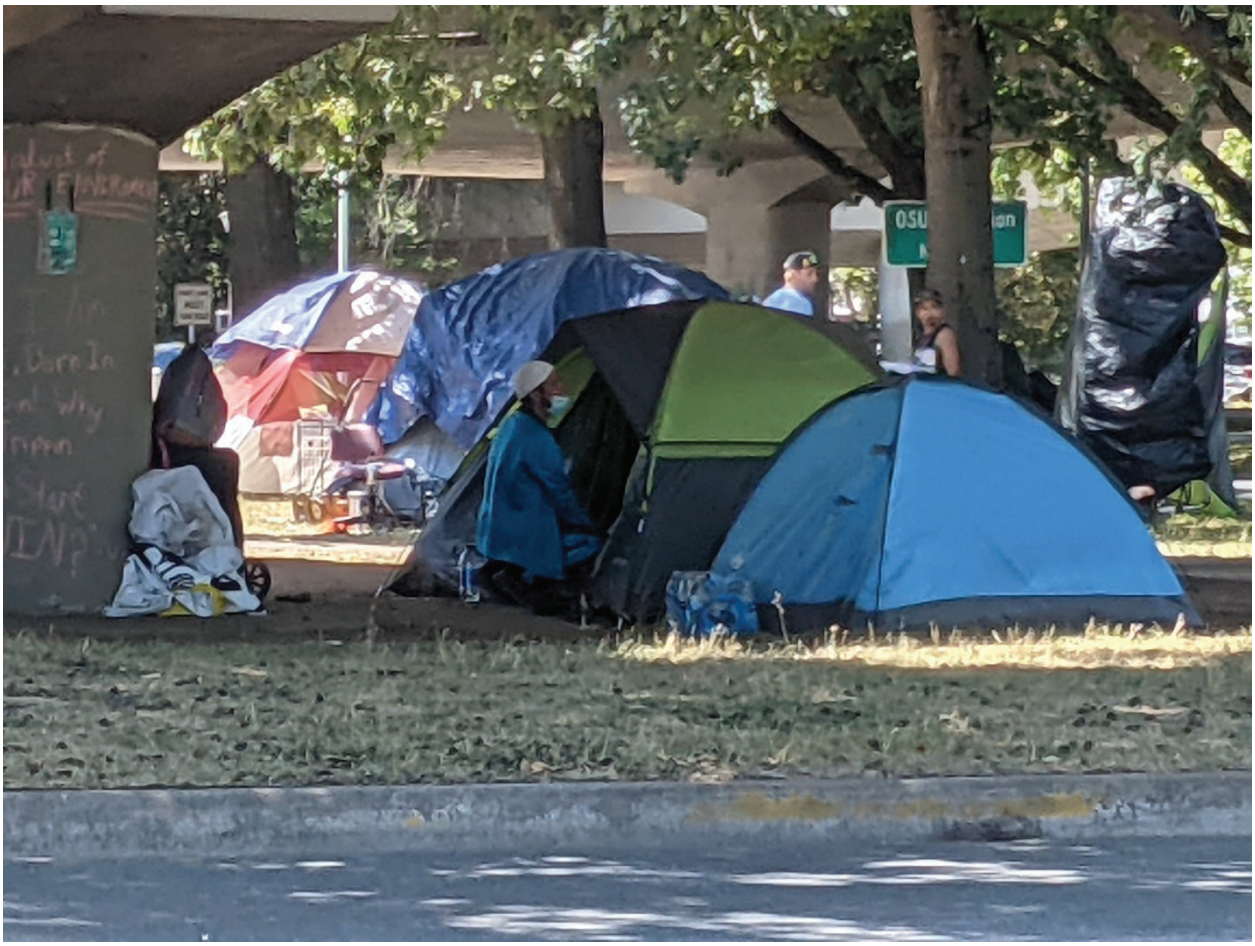
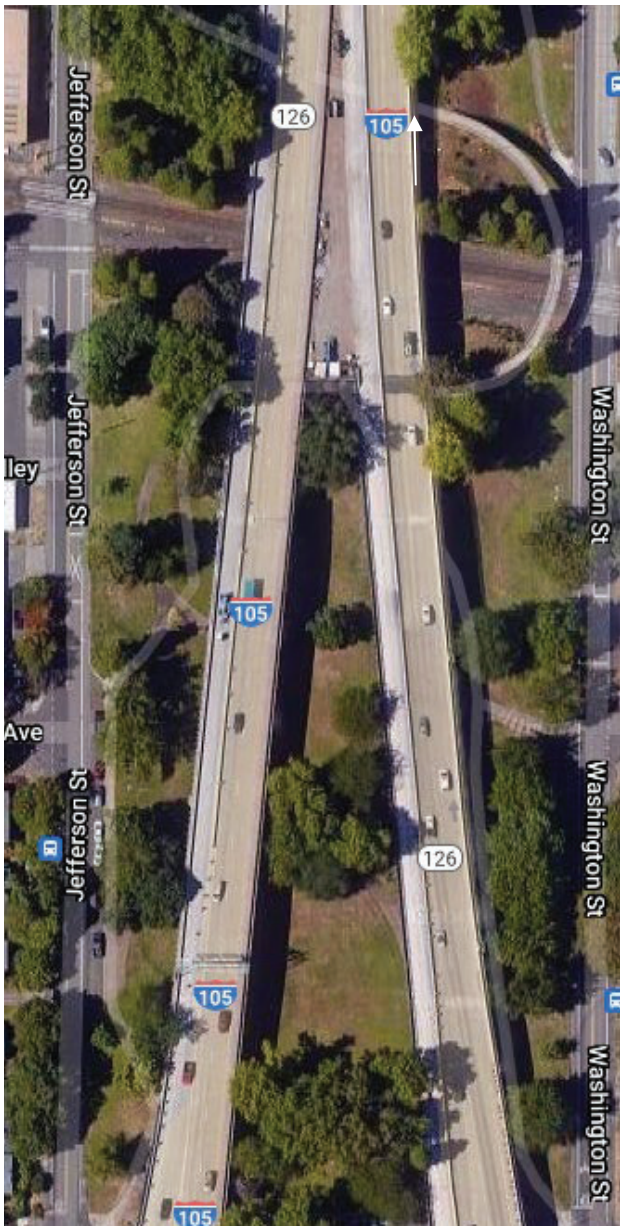


Figure 2



2. The person to be searched is Brandon Knight, aka Ibrahim Al-Amreeki, DOB: xx/xx/1994. Knight is depicted below.

3. The backpack to be searched is a small to medium-sized black backpack on or near the person of Brandon Knight or in or near the Premises. The backpack was observed to be adorned with bungee cords used for securing additional items to the exterior of the backpack, and at least one object—appearing to be a pole or bar—was attached to the bungee cords attached to the backpack and protruding approximately one foot from the backpack. Knight was last observed wearing the black backpack on July 6, 2021.

ATTACHMENT B

Items to Be Seized

The items to be searched for, seized, and examined, are those items on the Premises, a tent, a backpack, and Knight's person, as specified in attachment A and located in the Washington Jefferson Park, at 150 Jefferson St, Eugene, OR, 97402, that contain evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code (U.S.C.), Section 875(c) (transmitting threatening communications in interstate commerce. The items to be seized cover the period of June 11, 2021 through the date of the execution of the search warrant.

1. The items referenced above to be searched for, seized, and examined are as follows:

   a. Computers, storage media, or digital devices used to commit the violations described above.

   b. Communications, correspondence, information, records, documents, data, images, audio, video, social media, websites, and other print or electronic information pertaining to researching or planning to kill, injure, harass, or intimidate another person, or place persons under surveillance.

   c. Communications between Knight and AV1.

   d. Communications between Knight and anyone else regarding AV1.

   e. Information regarding Knight's feelings toward AV1 and information about any plans regarding AV1.

   f. Any physical or electronic notes regarding AV1.

g. Knives, blades, firearms and other dangerous weapons and ammunition.

h. Calendar entries, notes, documents, location data, browsing history, cookies, metadata and other records or information regarding Knight's location(s), or intended location(s).

i. Any records or information regarding internet usage, including browsing history, cookies, metadata and other records or information, relating to images, videos, or other media used for planning to kill, injure, harass, or intimidate another person, or place persons under surveillance.

j. Records containing screen names, usernames, and e-mail addresses, and identities assumed for the purposes of communication on the internet. These records may include billing and subscriber records, chat room logs, social media applications, e-mail messages or emails in draft form.

k. Records and information related to interstate travel or travel within the State of Oregon.

l. Envelopes, stamps, computer paper, printer, hand-written documents, and handwriting instruments, including pens, markers, or pencils.

m. Information regarding Knight's mental state and mental health

2. As used in this attachment, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing

devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter "Computer"):

a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c. Evidence of the lack of such malicious software.

d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.

e. Evidence indicating the Computer user's state of mind as it relates to the

crime under investigation.

f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.

h. Evidence of the times the Computer was used.

i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.

j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.

k. Records of or information about Internet Protocol addresses used by the Computer.

l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

n. Routers, modems, and network equipment used to connect computers to the Internet.

Search Procedure

4. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will

seal any image of the computer and storage media, absent further authorization from the Court.

8. The government may retain the computer and storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

9. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.